YOUTH SERVICES
POLICY

Title: Internet and Email Usage **Next Annual Review Date:** 04/30/2016	**Type:** A. Administrative **Sub Type:** 5. Information Services **Number:** A.5.6
	Page 1 **of** 5
References: Office of Information (OIT) Technology Standards IT STD-003 (Enterprise Applications: Electronic Messaging), IT STD-005 (Personal Computing: Browser/Viewer/Plug-Ins) IT STD-006 (Enterprise Systems: LAN Server Operating System/Network Operating System), IT STD-015 (Network: Public Web Site Domain Name Standard/and implications for E-Mail Address Standard); Office of Information Technology Policy IT POL 1-20 (Acceptable Internet/Email use); and YS Policy Nos. A.1.4 “Investigative Services”, A.2.1 “Employee Manual”, A.2.17 “Employee Suspensions: Pending Investigation, Enforced Annual Leave, Pending Criminal Proceedings”, and A.5.1 “Access to, Security of, and Use of Information Technology Resources and Mobile/Cellular/Smartphone Devises” and A.5.9 "Social Networking"	
STATUS: Approved	
Approved By: *Mary L. Livers, Deputy Secretary*	**Date of Approval:** 04/30/2015

I. AUTHORITY:

Deputy Secretary of Youth Services (YS) as contained in La. R.S. 36:405. Deviation from this policy must be approved by the Deputy Secretary.

II. PURPOSE:

To establish parameters for all employees listed below under APPLICABILITY regarding state-provided Internet and email usage.

III. APPLICABILITY:

All employees of YS, as well as contract personnel whose access to or use of Internet or email services is funded by YS or is available through equipment owned or leased by YS.

Each Unit Head is responsible for ensuring that all necessary procedures are in place to comply with the provisions of this policy.

IV. DEFINITIONS:

Access - Means to program, to execute programs on, to communicate with, store data in, retrieve data from, or otherwise make use of any resources, including data or programs, of a computer, computer system, or computer network.

Computer Equipment - Includes computer file servers, desktop/notebook computers, electronic data communications equipment, personal digital assistants (PDA), Blackberries and Smartphones.

Human Capital Management System (HCM) - A system that captures transactions involving state funds which was formerly performed by the Integrated Statewide System (ISIS).

Social Networks - On-line internet activity, all of which is trackable and traceable, and usually permanent. On-line social networks include blogs, chat rooms, message boards, discussion groups, email, texting, etc. where an employee writes/posts comments, or is a member of professionally or personally, including but not limited to, MySpace, Face book, Twitter, YouTube, Linkedin, or any such network now in existence or created in the future (refer to YS Policy No A.5.9).

Unauthorized Email Access -The ability to view, send, receive, modify, delete, print or copy an email where the individual gaining access does not have the right or the need to access the email.

Unauthorized Internet Activities - Accessing web sites for non YS-related purposes. Also included is downloading of information, files and/or programming using file transport protocol (FTP) or any other downloading of utilities.

Unauthorized Internet Use - Having access to the Internet where the individual gaining access does not have the right or the need to use the Internet. This includes access and unauthorized viewing of web-based data files that include youth information.

Unit Head - Deputy Secretary, Facility Directors and Regional Managers.

YS Central Office - Offices of the Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretary, General Counsel, Regional Directors, and their support staff.

V. POLICY:

It is the Deputy Secretary's policy that access to the Internet and email capabilities enhances productivity, staff communication, and the business functions of YS. Internet and email usage shall be for official business only. (Pursuant to IT POL 1-20, acceptable use of the internet and email is to provide and facilitate official state business, to use for professional society, university association, government advisory, or standards activities related to the user's employment-related professional/vocational discipline and other uses not in violation of this policy allowed or required by agency policy.)

Brief, incidental use of the Internet not on a recurring or regular basis and not related to personal business is permitted.

Access to pornographic or similar Internet web sites and all other similar uses are strictly prohibited at all times. Users may not download, transmit, display, or store any image or document using the agency system or resource that violates federal, state or local laws and regulations, executive orders, policies, procedures, standards or guidelines. An abuse of the privilege of Internet or email use may result in disciplinary action (refer to YS Policy No A.2.1).

All employees having Internet and email capabilities are responsible for preventing unauthorized access, including remote access to individual, password-protected email accounts by nonemployees or other unauthorized individuals.

Each employee is personally responsible for any on-line activity conducted with a YS/OJJ email address. The YS/OJJ email address attached to any employee's name implies that the employee is acting on YS/OJJ's behalf. In addition, employees are prohibited from posting comments/pictures that includes racist or discriminatory remarks, and defamatory or derogatory comments regarding YS/OJJ (refer to YS Policy No. A.5.9).

Staff Lotus Notes and Microsoft Outlook email signatures shall consist of the employee's name, title, work address, telephone and fax numbers only (refer to Section VIII.A of this policy).

Computer virus software with the latest virus subscription updates shall be installed on all computers that have Internet and/or email capabilities by Public Safety Services (PSS) IT.

An employee's email account shall be temporarily disabled when the employee is placed on enforced leave during an investigation, until the investigation is concluded, and if applicable the employee's laptop shall also be confiscated to alleviate access to OJJ databases.

VI. INTERNET APPROVAL PROCEDURES:

A. An employee may request internet access by completing and submitting the "Request for Internet Access" form [see Attachment A.5.6 (a)] to the Unit Head.

B. The Unit Head is responsible for approving the "Request for Internet Access", attaching the form to a URAC request, and forwarding the request to designated YS staff for approval.

C. Designated YS staff shall forward the URAC request with the attached "Request for Internet Access" form to the PSS IT Director.

D. The PSS IT Director shall provide final authorization and ensure that the employee receives the appropriate level of internet access.

VII. INTERNET PROCEDURES:

A. Internet access is granted only to employees who need access to perform their job duties. Because of the agency use of email as a communication mechanism, restrictions on Internet or email accounts are determined by the Unit Head.

Two levels of Internet access are available. One level is very restrictive, limiting employees to a small number of web sites. Additional sites can be added at the request of the Unit Head. This very restrictive level is appropriate for employees who need access to information only available via the web, such as the Human Capital Management (HCM) help site for timekeepers. The second level of Internet access is less restrictive and provides more flexibility for those employees needing broader access to the Internet.

B. Microsoft Internet Explorer, the State's standard web browser, shall be used for accessing web sites and services. All Internet usage will be routed through the YS computer network. Access to personal web sites and services are automatically blocked (i.e. Gmail, Hotmail, Yahoo, Face book, My Space, iTunes, etc.). All Internet usage is tracked and any questionable usage shall be reported by the PSS IT Director to the Deputy Secretary for disposition.

C. YS shall have one official web site: **www.ojj.la.gov**. The web site may include links to individual unit web sites. All information posted on the web site must have prior approval from the Undersecretary/designee. Web content may be any information that is clearly identified as public record. Web sites shall be designed to operate on both high-speed and low-speed Internet connections.

VIII. EMAIL PROCEDURES:

A. Since it is clear that YS/OJJ email addresses attached to any employee's name is reflecting that the employee is acting on YS/OJJ's behalf, it is not appropriate for employees to put personal comments/statements above or below the signature line of their emails. Therefore, Lotus Notes and Microsoft Outlook email signatures shall consist of the employee's name, title, work address, telephone and fax numbers only as required under Section V. of this policy.

B. All emails shall be sent and received using PSS and YS approved email system.

C. All emails sent to or received by YS employees shall be scanned for computer viruses by the PSS computer system. The system will reject emails detected with a computer virus. Email attachments received from outside individuals should not be opened or detached unless it is from a known and trusted source. Such attachments may contain computer viruses.

D. Email is not designed for long-term document storage. Each employee shall have an electronic mailbox with limited data storage. Emails that must be retained long-term should be archived to the employee's computer using the archiving feature.

E. Emails that may be considered part of the unit's records retention schedule should be printed, and a hard copy retained in the appropriate file.

F. Employees are responsible for the content of their emails. Because emails are not encrypted, there should be no expectation of confidentially or privacy. All email is subject to monitoring and auditing.

G. Pursuant to Section V of this policy, it is the Unit Head's responsibility to ensure the proper steps are taken through the URAC process to immediately disable the email account, and if applicable, retrieve the laptop, of an employee under investigation and placed on forced leave until the investigation is concluded. (Refer to YS Policy Nos. A.1.4 and A.2.17)

Previous Regulation/Policy Number: A.5.6
Previous Effective Date: 10/28/2014

Attachments/References:

A.5.6 (a) Request for Internet Access May2014.docx